Microsoft Exam Questions 70-744
Securing Windows Server 2016
NEW QUESTION 1
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. Computer1 connects to a home network and a corporate network. The corporate network uses the 172.16.0.0/24 address space internally. Computer1 runs an application named App1 that listens to port 8080. You need to prevent connections to App1 when Computer1 is connected to the home network. Solution: From Windows Firewall in the Control Panel, you add an application and allow the application to communicate through the firewall on a Private network.

Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
http://www.online-tech-tips.com/windows-10/adjust-windows-10-firewall-settings/

NEW QUESTION 2
Your network contains an Active Directory domain named contoso.com. The domain contains 1,000 client computers that run Windows 10. A security audit reveals that the network recently experienced a Pass-the-Hash attack. The attack was initiated from a client computer and accessed Active Directory objects restricted to the members of the Domain Admins group.
You need to minimize the impact of another successful Pass-the-Hash attack on the domain. What should you recommend?

A. Instruct all users to sign in to a client computer by using a Microsoft account.
B. Move the computer accounts of all the client computers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.
C. Instruct all administrators to use a local Administrators account when they sign in to a client computer.
D. Move the computer accounts of the domain controllers to a new organizational unit (OU). Remove the permissions to the new OU from the Domain Admins group.

Answer: C

Explanation:
https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard
NEW QUESTION 3
Your network contains an Active Directory domain named contoso.com. The domain contains four servers. The servers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Configuration</th>
<th>Operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC1</td>
<td>Domain controller</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>DC2</td>
<td>Domain controller</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>FS1</td>
<td>File server</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>FS2</td>
<td>File server</td>
<td>Windows Server 2012 R2</td>
</tr>
</tbody>
</table>

You need to manage FS1 and FS2 by using Just Enough Administration (JEA). What should you do before you can implement JEA?

A. Install Microsoft .NET Framework 4.6.2 on FS1
B. Upgrade DC1 to Windows Server 2016
C. Install Windows Management Framework 5.0 on FS2.
D. Deploy Microsoft Identity Manager (MIM) 2016 to the domain

Answer: C

Explanation:

The current release of JEA is available on the following platforms:
- Windows Server 2016 Technical Preview 5 and higher

FS1 is ready to be managed by JEA, but FS2 need some extra work to do, either upgrade it to Windows Server 2016 or install Windows Management Framework 5.0 installed.

NEW QUESTION 4
Note: This question b part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in a question apply only to that question.

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that runs Windows Server 2016. Server1 has a shared folder named Share1.

You need to ensure that all access to Share1 uses SMB Encryption. Which tool should you use?

A. File Explorer
B. Shared Folders
C. Server Manager
D. Disk Management
E. Storage Explorer
F. Computer Management
G. System Configuration
H. File Server Resource Manager (FSRM)

Answer: C

Explanation:
https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-inwindows-server-2012/
NEW QUESTION 5

Note: This question is part of a series of questions that use the same scenario. For your convenience, the scenario is repeated in each question. Each question presents a different goal and answer choices, but the text of the scenario is exactly the same in each question in this series.

Start of repeated scenario

Your network contains an Active Directory domain named contoso.com. The functional level of the forest and the domain is Windows Server 2008 R2. The domain contains the servers configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server name</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nano1</td>
<td>Nano Server</td>
</tr>
<tr>
<td>Nano2</td>
<td>Nano Server</td>
</tr>
<tr>
<td>Server2</td>
<td>File server that has a shared folder named DATA</td>
</tr>
<tr>
<td>Server3</td>
<td>DNS server that has a DNSSEC-signed zone named adatum.com</td>
</tr>
<tr>
<td>Server4</td>
<td>Hyper-V host</td>
</tr>
<tr>
<td>Server1</td>
<td>Application server</td>
</tr>
</tbody>
</table>

All servers run Windows Server 2016. All client computers run Windows 10.

You have an organizational unit (OU) named Marketing that contains the computers in the marketing department. You have an OU named Finance that contains the computers in the finance department. You have an OU named AppServers that contains application servers. A Group Policy object (GPO) named GP1 is linked to the Marketing OU. A GPO named GP2 is linked to the AppServers OU. You install Windows Defender on Nano1.

End of repeated scenario

You need to disable SMB 1.0 on Server2. What should you do?

A. From File Server Resource Manager, create a classification rule.
B. From the properties of each network adapter on Server2, modify the bindings.
C. From Windows PowerShell, run the Set-VMsmbClientConfiguration cmdlet.
D. From Server Manager, remove a Windows feature.

Answer: D

Explanation:

NEW QUESTION 6

Your network contains an Active Directory domain named contoso.com. You are deploying Microsoft Advanced Threat Analytics (ATA).

You create a user named User1.

You need to configure the user account of User1 as a Honeytoken account. Which information must you use to configure the Honeytoken account?

A. the SAM account name of User1
B. the Globally Unique Identifier (GUID) of User1
C. the SID of User1
D. the UPN of User1

Answer: C

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-prerequisites
A user account of a user who has no network activities. This account is configured as the ATA Honeytoken user.
To configure the Honeytoken user you need the SID of the user account, not the username.

ATA also enables the configuration of a Honeytoken user, which is used as a trap for malicious actors – any authentication associated with this (normally dormant) account will trigger an alert.
NEW QUESTION 7
HOTSPOT
Contoso.com trusts adatum.com.
You plan to deploy shielded virtual machines to Server1 and to configure Admin-trusted attestation on Server2. Which component should you install and which cmdlet should you run on Server2? To answer, select the appropriate options in the answer area.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Key for this question is Admin-trusted attestation or (AD mode) for guarded fabric “Server1.contoso.com”, while Server2.adatum.com is running the Host Guardian Service.


NEW QUESTION 8
HOTSPOT
You need to verify whether Control Flow Guard is enabled for App1.exe.
Which command should you run? To answer, select the appropriate options in the answer area.
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Control Flow Guard (CFG) is a highly-optimized platform security feature that was created to combat memory corruption vulnerabilities. By placing tight restrictions on where an application can execute code from, it makes it much harder for exploits to execute arbitrary code through vulnerabilities such as buffer overflows. To verify if Control Flow Guard is enabled for a certain application executable:

Run the dumpbin.exe tool (included in the Visual Studio 2015 installation) from the Visual Studio command prompt with the /headers and /loadconfig options: dumpbin.exe /headers /loadconfig test.exe.

The output for a binary under CFG should show that the header values include “Guard”, and that the load config values include “CF Instrumented” and “FID table present”.

NEW QUESTION 9

DRAG DROP

You configure Just Enough Administration (JEA).

You need to ensure that a non-administrator user can perform the following actions:
- Restart Internet Information Services (IIS)
- Restart a custom service named Service1.

How should you complete the role configuration file? To answer, select the appropriate options in the answer area.
A. Mastered
B. Not Mastered

Answer: A

Explanation:
VisibleExternalCommands = 'C:\Windows\system32\iisreset.exe'
VisibleCmdlets = @(Name 'Restart-service'; Parameters @(
Name = 'Name'; ValidateSet = 'Service1'))
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities

NEW QUESTION 10
HOTSPOT
Your network contains an Active Directory named contoso.com.
The domain contains the computers configured as shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server1</td>
<td>172.16.1.30</td>
</tr>
<tr>
<td>Computer1</td>
<td>172.16.10.60</td>
</tr>
<tr>
<td>Computer2</td>
<td>172.16.20.50</td>
</tr>
</tbody>
</table>

Server1 has a share named Share1 with the following configurations:-
Server1, Computer1, and Computer2 have the connection security rules configured as shown in follow:-

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ShareState</td>
<td>Online</td>
</tr>
<tr>
<td>AvailabilityType</td>
<td>NonClustered</td>
</tr>
<tr>
<td>ShareType</td>
<td>FileSystemDirectory</td>
</tr>
<tr>
<td>FolderEnumerationMode</td>
<td>Unrestricted</td>
</tr>
<tr>
<td>CachingMode</td>
<td>Manual</td>
</tr>
<tr>
<td>SmbInstance</td>
<td>Default</td>
</tr>
<tr>
<td>CATimeout</td>
<td>0</td>
</tr>
<tr>
<td>ConcurrentUserLimit</td>
<td>0</td>
</tr>
<tr>
<td>ContinuouslyAvailable</td>
<td>False</td>
</tr>
<tr>
<td>CurrentUsers</td>
<td>0</td>
</tr>
<tr>
<td>Description</td>
<td>:True</td>
</tr>
<tr>
<td>EncryptData</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Share1</td>
</tr>
<tr>
<td>Path</td>
<td>C:\Shares\Share1</td>
</tr>
<tr>
<td>Scoped</td>
<td>False</td>
</tr>
<tr>
<td>ScopeName</td>
<td></td>
</tr>
<tr>
<td>SecurityDescriptor</td>
<td>O: BAG: DUD: (A; OICI; FA; ; WD)</td>
</tr>
<tr>
<td>ShadowCopy</td>
<td>False</td>
</tr>
<tr>
<td>Special</td>
<td>False</td>
</tr>
<tr>
<td>Temporary</td>
<td>False</td>
</tr>
<tr>
<td>Volume</td>
<td>??\Volume\18eb1d3f-0000-0000-0000-501f00000000</td>
</tr>
<tr>
<td>PSComputerName</td>
<td></td>
</tr>
<tr>
<td>CimInstanceProperties</td>
<td>(AvailabilityType, CachingMode, CATimeout, ConcurrentUserLimit)</td>
</tr>
</tbody>
</table>

Please Select the correct statement as below:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
When Computer1 accesses Share1, SMB encryption will be used: YES
When Computer2 accesses Share1, SMB encryption will be used: YES
When Server1 accesses a shared folder on Computer1, IPSec encryption will be used: YES
When Server1 accesses a shared folder on Computer1, IPsec encryption will be used: NO
The shared folder “Share1” is configured with “EncryptData : True”, no matter which network the client resides, SMB 3 communication will be encrypted.
When Server1 access Computer1 over network, the original packet L3 IP Header is as follow: 172.16.1.30 –> 172.16.10.60
These traffic does not match the enabled IPsec rule “Rule2” nor “Rule3”, and the only matching rule “Rule1” is disabled. So, no IPsec encryption will be achieved.

NEW QUESTION 11
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. The network uses the 172.16.0.0/16 address space.
Computer1 has an application named App1.exe that is located in D:\Apps\. App1.exe is configured to accept connections on TCP port 8080.
You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.
Solution: You configure an inbound rule that allows the TCP protocol on port 8080, uses a scope of 172.16.0.0/16 for local IP addresses, and applies to a private profile.
Does this meet the goal?
A. Yes
B. No

Answer: B

Explanation:
“You need to ensure that App1.exe can accept connections only when Computer1 is connected to the corporate network.”, you should create the firewall rule for ‘Domain’ profile instead, not the ‘Private’ profile.

NEW QUESTION 12
Solution: From Windows PowerShell, you run the Disable-WindowsOptionalFeature cmdlet. Does this meet the goal?
A. Yes
B. No

Answer: B

Explanation:
On Client, the PowerShell approach (Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol)
On Server, the PowerShell approach (Remove-WindowsFeature FS-SMB1): Remove-WindowsFeature FS-SMB1

Guaranteed success with Our exam guides
visit - https://www.certshared.com
Even if SMB1 is removed, SMB2 and SMB3 could still run NTLM authentication! Therefore, answer is a "NO".

NEW QUESTION 13
You implement Just Enough Administration (JEA) on several file servers that run Windows Server 2016. The Role Capability file from a server named Server5 contains the following code.
```
VisibleCmdlets = 'Set-Acl',
    @{
        Name = 'Stop-Process'
        Parameters = @{ Name = 'Name'; ValidateSet = 'proc' }
    },
    'SmbShare\Set-*'
    'SmbShare\Get-*'
```
Which action can be performed by a user who connects to Server5?
A. Create a new file share.
B. Modify the properties of any share.
C. Stop any process.
D. View the NTFS permissions of any folder.

Answer: B

Explanation:
https://docs.microsoft.com/en-us/powershell/jea/role-capabilities Focus on the 3rd Visible Cmdlets in this question 'SmbShare\Set-*'
The PowerShell "SmbShare" module has the following "Set-*" cmdlets, as reported by "Get-Command -Module SmbShare" command:
```
Set-SmbBandwidthLimit
Set-SmbClientConfiguration
Set-SmbPathAcl
Set-SmbServerConfiguration
Set-SmbShare
```
The "Set-SmbShare" cmdlet is then visible on Server5's JEA endpoint, and allows JEA users to modify the properties of any file share.

NEW QUESTION 14
Your network contains an Active Directory forest named contoso.com. The forest functional level is Windows Server 2012. The forest contains 20 member servers that are configured as file servers. All domain controllers run Windows Server 2016. You create a new forest named contosoadmin.com. You need to use the Enhanced Security Administrative Environment (ESAE) approach for the administration of resources in contoso.com. Which two actions should you perform? Each correct answer presents part of the solution.
A. From the properties of the trust, enable selective authentication.
B. Configure contosoadmin.com to trust contoso.com.
C. Configure contoso.com to trust contosoadmin.com.
D. From the properties of the trust, enable forest-wide authentication.
E. Configure a two-way trust between both forest

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securingprivilegedaccess-reference-material#ESAE_BM
Trust configurations – Configure trust from managed forests(s) or domain(s) to the administrative forest
A one-way trust is required from production environment to the admin forest. This can be a domain trust or a forest trust. The admin forest/domain (contosoadmin.com) does not need to trust the managed domains/forests (contoso.com) to manage Active Directory, though additional applications may require a two-way trust relationship, security validation, and testing. Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

NEW QUESTION 15
The Job Title attribute for a domain user named User1 has a value of Sales Manager. User1 runs whoami /claims and receives the following output:
Kerberos support for Dynamic Access Control on this device has been disabled.

You need to ensure that the security token of User1 has a claim for Job Title. What should you do?

A. From Windows PowerShell, run the New-ADClaimTransformPolicy cmdlet and specify the -Name parameter
B. From Active Directory Users and Computers, modify the properties of the User1 account.
C. From Active Directory Administrative Center, add a claim type.
D. From a Group Policy object (GPO), configure KDC support for claims, compound authentication, and Kerberos armoring.

Answer: C

Explanation:
From the output, obviously, a claim type is missing (or disabled) so that the domain controller is not issuing tickets with the "Job Title" claim type.

NEW QUESTION 16

Your network contains an Active Directory forest named corp.contoso.com.

You are implementing Privileged Access Management (PAM) by using a bastion forest named priv.contoso.com.

You need to create shadow groups in priv.contoso.com. Which cmdlet should you use?

A. New-RoleGroup
B. New-ADGroup
C. New-PamRole
D. New-PamGroup

Answer: D

Explanation:

NEW QUESTION 17

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.

<table>
<thead>
<tr>
<th>Volume label</th>
<th>Volume letter</th>
<th>Size(TB)</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>C</td>
<td>4</td>
<td>NTFS</td>
</tr>
<tr>
<td>HRFiles</td>
<td>H</td>
<td>8</td>
<td>NTFS</td>
</tr>
<tr>
<td>SalesFiles</td>
<td>J</td>
<td>8</td>
<td>ReFS</td>
</tr>
<tr>
<td>DevFiles</td>
<td>K</td>
<td>10</td>
<td>NTFS</td>
</tr>
<tr>
<td>BackUp</td>
<td>L</td>
<td>6</td>
<td>ReFS</td>
</tr>
</tbody>
</table>

You need to encrypt DevFiles by using BitLocker Drive Encryption (BitLocker). Solution: You run the manage-bde.exe command and specify the –on parameter. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/managebde- on

NEW QUESTION 18

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this sections, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You manage a file server that runs Windows Server 2016. The file server contains the volumes configured as shown in the following table.
You need to encrypt DevFiles by using BitLocker Drive Encryption (BitLocker). Solution: You run the Lock-BitLocker cmdlet. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

References:

NEW QUESTION 19

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. The domain has Dynamic Access Control enabled.

Server1 contains a folder named C:\Folder1. Folder1 is shared as Share1.

You need to audit all access to the contents of Folder1 from Server2. The solution must minimize the number of event log entries.

Which two audit policies should you enable on Server1? Each correct answer presents part of the solution.

A. Global Object Access - File System
B. Object Access – Audit Detailed File Share
C. Object Access – Audit Other Object Access Events
D. Object Access – Audit File System
E. Object Access – Audit File Share

Answer: BE

Explanation:

References:

NEW QUESTION 20

HOTSPOT


You create a PAM role named Group1 as shown in the following exhibit.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

If Priv.User1 requests the Group1 PAM role at 07:00, [answer choice].

- the request will be denied
- Priv.User1 will be added to Group1 immediately
- Priv.User1 will be added to Group1 as soon as the request is approved
- Priv.User1 will be added to Group1 at 8:00

If Priv.User2 requests the Group1 PAM role at 09:00, [answer choice].

- the request will be denied
- Priv.User2 will be added to Group1 immediately
- Priv.User2 will be added to Group1 as soon as the request is approved
- Priv.User2 will be added to Group1 at 8:00

A. Mastered  
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 21

Guaranteed success with Our exam guides
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

70-744 Practice Exam Features:

* 70-744 Questions and Answers Updated Frequently
* 70-744 Practice Questions Verified by Expert Senior Certified Staff
* 70-744 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 70-744 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click Order The 70-744 Practice Test Here